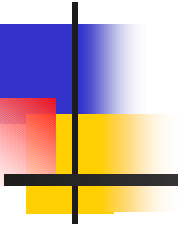# Multiprotocol Label Switching Architecture & LDP

- Introduction
- MPLS Basics
- LDP Procedures
- LDP Specification

MPLS&LDP->Introduction

- ## Conventional network forwarding

  Each router analyzes the coming packet's header and independently chooses a next hop. Routing algorithm and adequate speed are prerequisite.

- ## MPLS forwarding

  All forwarding is driven by the labels, no header analysis needed. Once a packet enters a network, it's assigned a label. Each router forwards packets according their labels.

MPLS&LDP->Introduction

- **Advantages over conventional routing**

1. Router can use any information in determining label assignment, not limited to packet header;

2. How to distribute labels may become more and more complicated, without any impact on the routers that merely forward labeled packets.

3. A label can be used to represent a pre-chosen route so that the identity of explicit route need not be carried with the packet.

4. Mutiprotocol: its techniques are applicable to ANY network layer protocol.

5. Etc.

MPLS&LDP->Introduction

- ## Terminology. Some important terms.

FEC(forwarding equivalence class)   a group of IP packets which are forwarded in the same manner (e.g., over the same path, with the same forwarding treatment)

LSR(label switching router)   an MPLS node which is capable of forwarding native Layer 3 packets

label swap   the basic forwarding operation consisting of looking up an incoming label to determine the outgoing label, encapsulation, port, and other data handling information.

MPLS domain   a contiguous set of nodes which operate MPLS routing and forwarding and which are also in one Routing or Administrative Domain
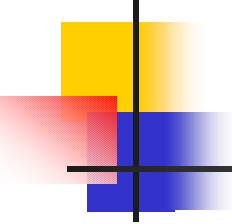
- ## FECs

  Each FEC is specified as a set of one or more FEC elements. Each FEC element identifies a set of packets which may be mapped to the corresponding LSP.

  1. Address Prefix. This element is an address prefix of any length from 0 to a full address, inclusive.

  2. Host Address. This element is a full host address.

MPLS&LDP->MPLS Basics

- Labels

- Packet forward

- Route selection

- Tunnels and Hierarchy

- Multiprotocol

MPLS&LDP->MPLS Basics->Labels

A label is a short, fixed length, locally significant identifier which is used to identify a FEC. The label which is put on a particular packet represents the FEC to which that packet is assigned.

Most commonly, a packet is assigned to a FEC based (completely or partially) on its network layer destination address. However, the label is never an encoding of that address.

MPLS&LDP->MPLS Basics->Labels

Ru → Rd
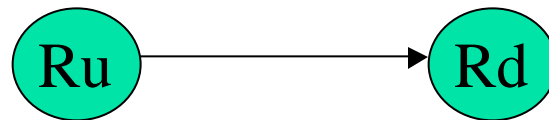
Upstream LSR   Downstream LSR

Agreement: "binding" label L to FEC F for packets moving from Ru to Rd.

So, L becomes Ru's "outgoing label" representing FEC F, and L becomes Rd's "incoming label" representing FEC F. Note that L is an arbitrary value whose binding to F is local to Ru and Rd.

- *Label Assignment and Distribution*

  The decision to bind a particular label L to a particular FEC F is made by the LSR which is DOWNSTREAM with respect to that binding. The downstream LSR then informs the upstream LSR of the binding.

MPLS&LDP->MPLS Basics->Labels

- A label distribution protocol is a set of procedures by which one LSR informs another of the label/FEC bindings it has made.

- The label distribution protocol also encompasses any negotiations in which two label distribution peers need to engage in order to learn   of each other's MPLS capabilities.

- THE ARCHITECTURE DOES NOT ASSUME THAT THERE IS ONLY A SINGLE LABEL DISTRIBUTION PROTOCOL. E.g., [MPLS-BGP], [MPLS-RSVP], [MPLS-RSVP-TUNNELS], [MPLS-LDP], [MPLS-CR-LDP].

Examine the label of packet

Unlabeled

labeled

Determine FEC

Invalid label

ILM

Discard

No outgoing label
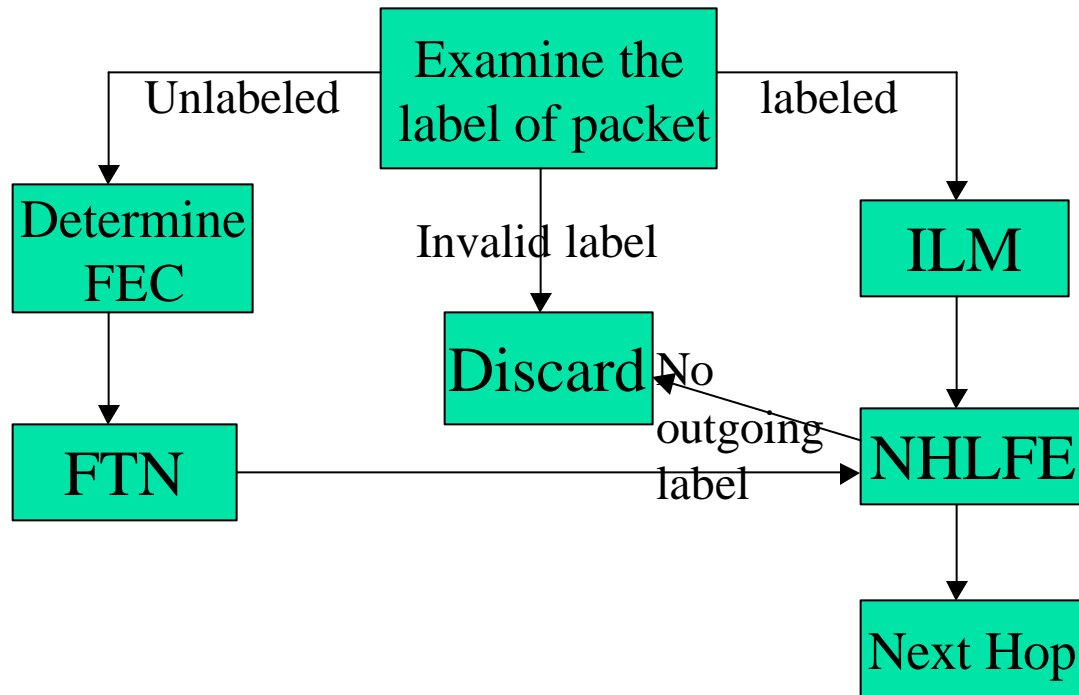
FTN

NHLFE

Next Hop

Fig 1. Procedures to forward a packet

MPLS&LDP->MPLS Basics-> Packet forward

- ILM(Incoming Label Map)
  Maps each incoming label to a set of NHLFEs.
- NHLFE(Next Hop Label Forwarding Entry)
  It contains the following information:
  1. the packet's next hop
  2. the operation to perform on the packet's label stack; this is
     one of the following operations:
  - a) replace the label at the top of the label stack with a
       specified new label
  - b) pop the label stack
  - c) replace the label at the top of the label stack with a
       specified new label, and then push one or more specified
       new labels onto the label stack.
  It may also contain some other information

- ## FTN(FEC-to-NHLFE)

  The FTN maps each FEC to a set of NHLFEs. It is used

  when forwarding packets that arrive unlabeled, but which
  are to be labeled before being forwarded.

- ## Determine unlabeled packet's FEC

  LSR analyzes the layer network header to make decision.
  How to analyze is beyond the scope of architecture.

MPLS&LDP->MPLS Basics-> Packet forward

- ## Invalid Incoming Labels

  when a labeled packet is received with an invalid incoming label, it MUST be discarded, UNLESS it is determined by some means (not within the scope of the MPLS architecture) that forwarding it unlabeled cannot cause any harm.

- ## Lack of Outgoing Label

  Unless it can be determined that neither of these situations applies, the only safe procedure is to discard the packet.

  - If the packet has been following an explicitly routed LSP, this could result in a loop.

  -The packet's network header may not contain enough information to enable this particular LSR to forward it correctly.
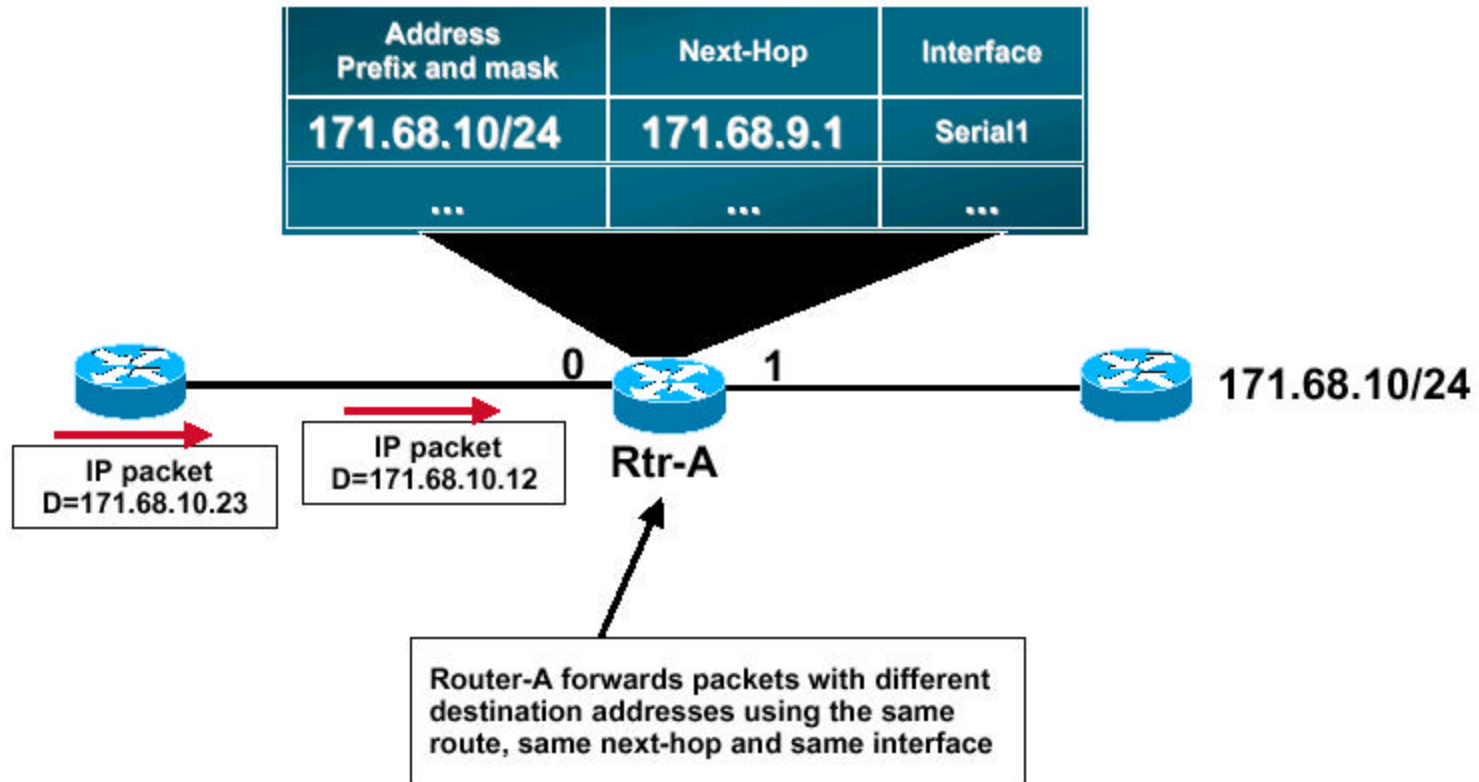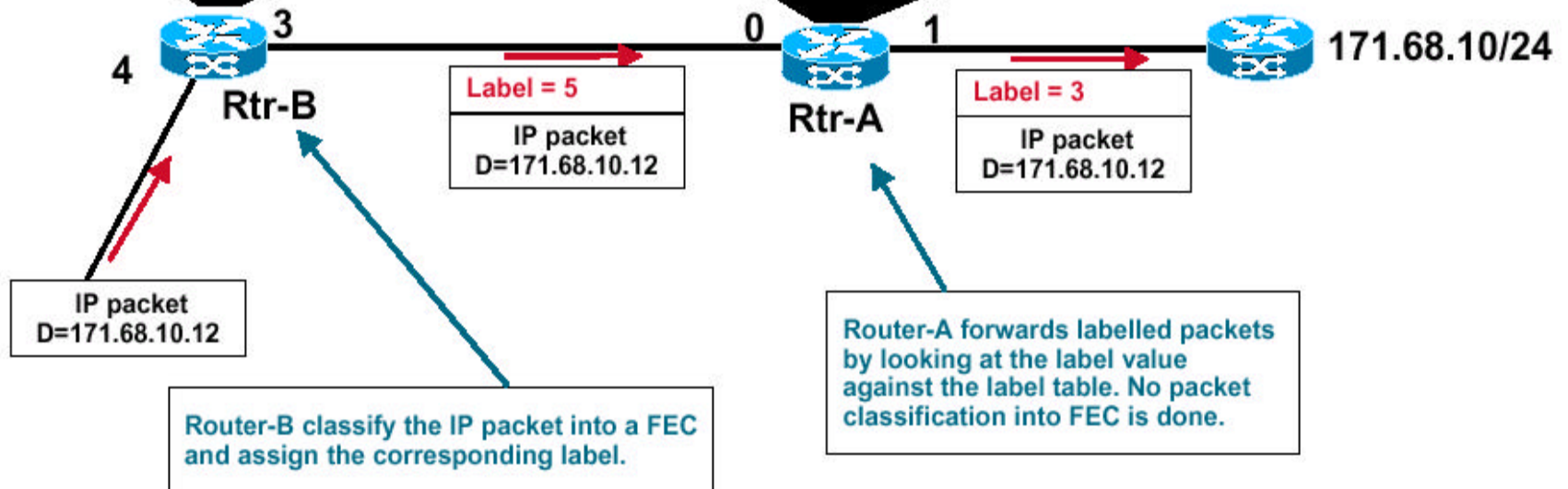
MPLS&LDP->MPLS Basics-> Packet forward

In I/F	In Lab	Address Prefix	Out I/F	Out Lab
4	x	171.68.10	3	5
...	...	...	...	...

In I/F	In Lab	Address Prefix	Out I/F	Out Lab
0	5	171.68.10	1	3
...	...	...	...	...

171.68.10/24

Rtr-B

Rtr-A

Label = 5
IP packet
D=171.68.10.12

Label = 3
IP packet
D=171.68.10.12

IP packet
D=171.68.10.12

Router-B classify the IP packet into a FEC and assign the corresponding label.

Router-A forwards labelled packets by looking at the label value against the label table. No packet classification into FEC is done.

- ## Hop by hop routing

  Allows each node to independently choose the next hop for each FEC. This is the usual mode today in existing IP networks. A "hop by hop routed LSP" is an LSP whose route is selected using hop by hop routing.

- ## Explicit routing

  A single LSR, generally the LSP ingress or the LSP egress, specifies several (or all) of the LSRs in the LSP. Explicit routing may be useful for a number of purposes, such as policy routing or traffic engineering.
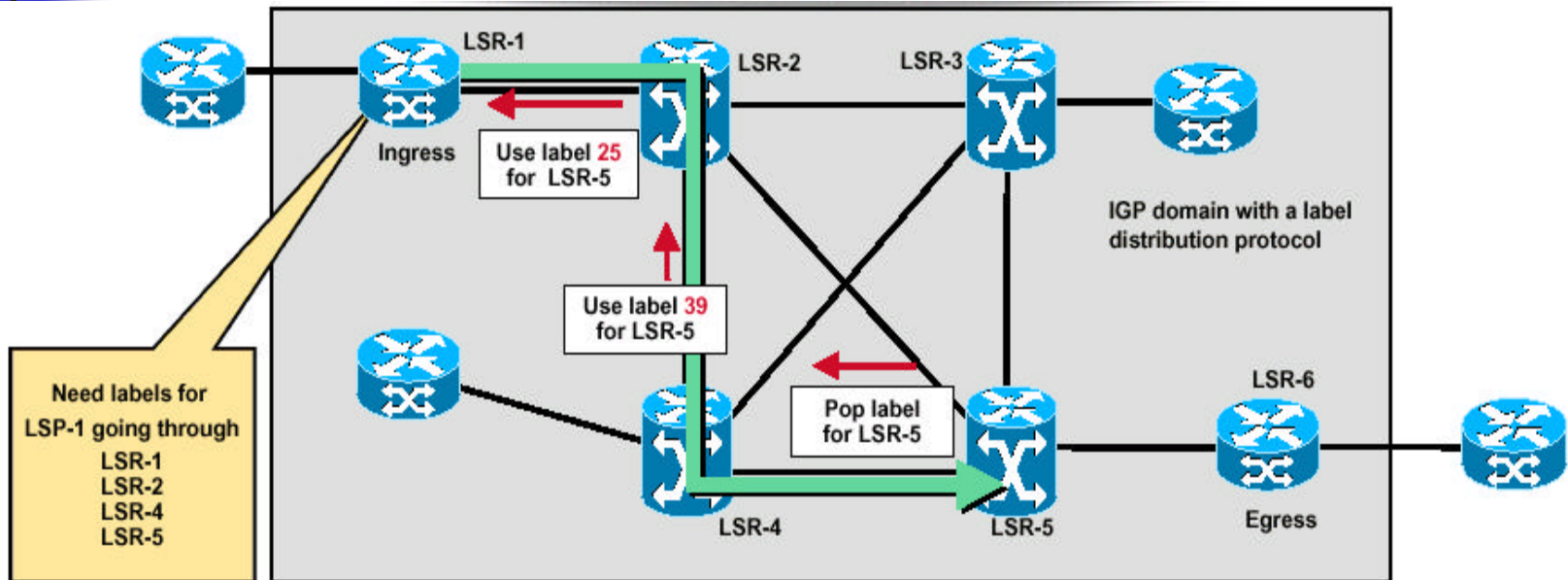
- **LSR-1 request an explicit LSP to LSR-6:**

  LSR1, LSR-2, LSR-4, LSR-5, LSR-6

- The request travels hop-by-hop and when it reaches the egress point labels are advertised back to the ingress LSR
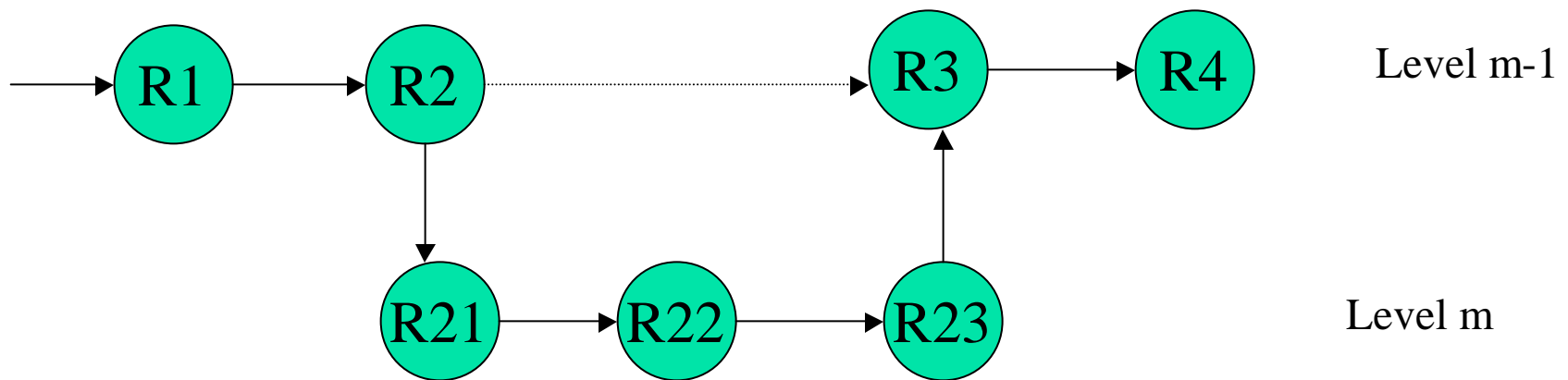
Fig. 2. Tunnels and Hierarchy

MPLS&LDP->MPLS Basics-> Tunnels&Hierarchy

- ## Hop-by-Hop Routed Tunnel

  If a Tunneled Packet follows the Hop-by-hop path from Ru to Rd, we say that it is in an "Hop-by-Hop Routed Tunnel" whose "transmit endpoint" is Ru and whose "receive endpoint" is Rd.

- ## Explicitly Routed Tunnel

  If a Tunneled Packet travels from Ru to Rd over a path other than the Hop-by-hop path, we say that it is in an "Explicitly Routed Tunnel" whose "transmit endpoint" is Ru and whose "receive endpoint" is Rd. For example, we might send a packet through an Explicitly Routed Tunnel by encapsulating it in a packet which is source routed.

- Labels for RSVP

When RSVP is used to set up resource reservations for particular

flows, it can be desirable to label the packets in those flows, so

that the RSVP does not need to be applied at each hop. It can be argued
that having RSVP distribute the labels as part of its path/reservation
setup process is the most efficient method of

distributing labels for this purpose.

- **Labels for Explicitly Routed LSPs**

  In some applications of MPLS, particularly those related to traffic engineering, it is desirable to set up an explicitly routed path, from ingress to egress. It is also desirable to apply resource reservations along that path.

  One can imagine two approaches to this:

  - Start with an existing protocol that is used for setting up resource reservations, and extend it to support explicit routing and label distribution.

  - Start with an existing protocol that is used for label distribution, and extend it to support explicit routing and resource reservations.

MPLS&LDP-> LDP Procedures

1. ## Downstream LSR: Distribution Procedure

   The Distribution Procedure is used by a downstream LSR to determine when it should distribute a label binding for a particular address prefix to its label distribution peers.

2. ## Upstream LSR: Request Procedure

   The Request Procedure is used by the upstream LSR for an address prefix to determine when to explicitly request that the downstream LSR bind a label to that prefix and distribute the binding.

MPLS&LDP-> LDP Procedures

3.   Upstream LSR: Release Procedure

   Suppose that Rd is an LSR which has bound a label to address prefix

   X, and has distributed that binding to LSR Ru. If Rd does not happen to be Ru's L3 next hop for address prefix X, or has ceased to be Ru's L3 next hop for address prefix X, then Ru will not be using the label. The Release Procedure determines how Ru acts in this case.

4.   Upstream LSR: labelUse Procedure

   Suppose Ru is an LSR which has received label binding L for address prefix X from LSR Rd, and Ru is upstream of Rd with respect to X.

   Ru will make use of the binding if Rd is Ru's L3 next hop for X. The labelUse Procedure determines just how Ru makes use of Rd's binding.

MPLS&LDP-> LDP Procedures

- ## Security Considerations

  Some routers may implement security procedures which depend on the network layer header being in a fixed place relative to the data link layer header. The MPLS generic encapsulation inserts a shim between the data link layer header and the network layer header. This may cause any such security procedures to fail.

  An MPLS label has its meaning by virtue of an agreement between the LSR that puts the label in the label stack, and the LSR that interprets that label (the "label reader"). If labeled packets are accepted from untrusted sources, or if a particular incoming label is accepted from an LSR to which that label has not been distributed, then packets may be routed in an illegitimate manner.